

Sum-Product Type Estimates for Subsets of Finite Valuation Rings

Esen Aksoy Yazici

January 30, 2017

Abstract

Let R be a finite valuation ring of order q^r . Using a point-plane incidence estimate in R^3 , we obtain sum-product type estimates for subsets of R . In particular, we prove that for $A \subset R$,

$$|AA + A| \gg \min \left\{ q^r, \frac{|A|^3}{q^{2r-1}} \right\}.$$

We also show that if $|A + A||A|^2 > q^{3r-1}$, then

$$|A^2 + A^2||A + A| \gg q^{\frac{r}{2}} |A|^{\frac{3}{2}}.$$

1 Introduction

The classical sum-product estimates in additive combinatorics is about comparing the size $|A|$ of finite subset A of a ring R with $|A + A|$ and $|A.A|$ and more generally with $|F(A)|$ for some function F of A . It is expected that either $|A + A|$ or $|A.A|$ has large growth compared to $|A|$, unless A is close to being a subring of R . A variant of this problem arises considering the similar questions for combinations of different subsets of R . Sum-product variant questions have been of great interest and was considered in many different context by various authors in the literature. For an extensive exploration of the subject, we refer the reader [2–8, 10, 12, 13] and the references therein.

The growth estimates in finite field setting was recently studied by Aksoy Yazici, Murphy, Rudnev and Shkredov in [2]. The main tool in that paper was a point-plane incidence estimate in FP^3 given by Rudnev in [9], where $F = \mathbb{F}_q$ is a finite field of order q , and FP^3 is the 3-dimensional projective space over F . The method was to consider the number of solution of an energy equation in F^3 , which was called as collision, as a point-plane incidence in the same space and then applying the aforementioned incidence bound.

In [11], Thang and Vinh used a graph theoretical approach to obtain a point-line incidence bound in R^2 , where R is a finite valuation ring of order q^r . They later used this estimate to improve and generalize the triangle area result given in [1] for \mathbb{Z}_q^2 to R .

Here in this paper, we aim to use the graph theoretical approach similar to the Thang and Vinh's argument and obtain a point-plane incidence bound in R^3 . We then utilize it with an analog set up in [2] to get the following sum-product estimates for subsets of finite valuation rings.

1.1 Notation.

Throughout $X \ll Y$ means that there exists an absolute constant c such that $X < cY$, and " \gg " is defined in a similar way. For a ring R , we denote the set of units as R^* and the set of nonunits as R^0 .

Let A and B be nonempty subsets of R . The sum set is defined as

$$A + B = \{a + b : a \in A, b \in B\}.$$

Similarly, the product set is

$$AB = \{a.b : a \in A, b \in B\}$$

and

$$A^n = \{a^n : a \in A\}.$$

1.2 Statement of Main Results

In the following two theorems, we modify sum-product results in [2] over finite fields to prove their analogs over finite valuation rings.

Theorem 1.1. *Let R be a finite valuation ring of order q^r and A, B, C be subsets of R . Then,*

$$|BA + C| \gg \min \left\{ q^r, \frac{|A||B||C|}{q^{2r-1}} \right\}.$$

In particular,

$$|AA + A| \gg \min \left\{ q^r, \frac{|A|^3}{q^{2r-1}} \right\},$$

so that if $|A| > q^{r-\frac{1}{3}}$, then $|AA + A| \gg q^r$

Theorem 1.2. *Let R be a finite valuation ring of order q^r . Let A be subset of R . If $|A + A||A|^2 > q^{3r-1}$, then*

$$|A^2 + A^2||A + A| \gg q^{\frac{r}{2}} |A|^{\frac{3}{2}}.$$

2 Proof of Theorem 1.1

For the Proof of Theorem 1.1 we will need the following two results from spectral graph theory.

Lemma 2.1. [11, Lemma 2.1] *Suppose G is a bipartite graph with parts A, B such that the vertices in A all have degree a and the vertices in B all have degree b . For any two sets $X \subset A$ and $Y \subset B$, the number of edges between X and Y , $e(X, Y)$, satisfies*

$$\left| e(X, Y) - \frac{a}{|B|} |X| |Y| \right| \leq \lambda_3 |X|^{\frac{1}{2}} |Y|^{\frac{1}{2}}$$

where λ_3 is the third eigenvalue of G .

Erdős-Renyi bipartite graphs $E_{q,d}(R) = (A \cup B, E)$ over finite valuation rings are defined as follows: The vertices of $E_{q,d}(R)$ are given by $[x]$, where $x \in R^d \setminus (R^0)^d$ and $[x]$ is equivalent to $[y]$ if and only if $x = ty$ for some $t \in R^*$. There is an edge between $[x]$ and $[y]$ if and only if $x \cdot y = 0$

Theorem 2.2. [11, Theorem 2.4] *The cardinality of each vertex part of $E_{q,d}(R)$ is $q^{(d-1)(r-1)} \frac{(q^d-1)}{q-1}$, $\deg(A) = \deg(B) = q^{(d-2)(r-1)} \frac{(q^{d-1}-1)}{q-1}$, and the third eigenvalue $\lambda_3 \leq q^{\frac{1}{2}(d-2)(2r-1)}$.*

In the proof of Theorem 1.1 we will use the following incidence theorem between points and planes in R^3 , which is analogous to the point-line incidence bound in R^2 given in [11, Theorem 4.2].

Theorem 2.3. *Let R be a finite valuation ring of order q^r . Let Q be a set of points in R^3 and Π be a set of planes in R^3 . Then the number of incidences $|I(Q, \Pi)|$ between Q and Π satisfies*

$$\left| |I(Q, \Pi)| - \frac{1}{q^{r-1}} \frac{(q^2 + q + 1)}{(q^3 + q^2 + q + 1)} |Q| |\Pi| \right| \leq q^{2r-1} |Q|^{\frac{1}{2}} |\Pi|^{\frac{1}{2}} \quad (2.1)$$

Hence

$$|I(Q, \Pi)| \leq \frac{1}{q^r} |Q| |\Pi| + q^{2r-1} |Q|^{\frac{1}{2}} |\Pi|^{\frac{1}{2}}.$$

Proof. We can identify the point $(x_1, x_2, x_3) \in Q$ with $[x_1, x_2, x_3, 1] \in E_{q,4}(R)$, and the plane $ax + by + cz = d$ in Π , $(a, b, c, d) \in R^4 \setminus (R^0)^4$, with $[a, b, c, -d] \in E_{q,4}(R)$. Therefore we will identify Q with Q' and Π with Π' , where $Q' = \{[x_1, x_2, x_3, 1] : (x_1, x_2, x_3) \in Q\}$ and $\Pi' = \{[a, b, c, -d] : ax + by + cz = d \text{ in } \Pi\}$. Note that $|Q| = |Q'|$ and $|\Pi| = |\Pi'|$.

Then it clearly follows that the number of incidences between Q and Π is equal to the number of edges between Q' and Π' in the Erdős-Renyi graph $E_{q,4}(R)$. By Theorem 2.2, the cardinality of each vertex part of $E_{q,4}(R)$ is $q^{3(r-1)}(q^3 + q^2 + q + 1)$, $\deg(A) = \deg(B) =$

$q^{2(r-1)}(q^2 + q + 1)$ and the third eigenvalue λ_3 of $E_{q,4}$ is at most q^{2r-1} . From Lemma 2.1, (2.1) follows which implies that

$$|I(Q, \Pi)| \leq \frac{1}{q^r} |Q| |\Pi| + q^{2r-1} |Q|^{\frac{1}{2}} |\Pi|^{\frac{1}{2}} \quad (2.2)$$

and completes the proof. \square

For the proof of Theorem 1.1, we use a similar set up given in [2] for the sum-product type estimates over finite fields. For completeness, we recall the notation and give the proof accordingly.

Let $P \subset R^2 \setminus \{(0, 0)\}$. Define the set of lines

$$L = L_P = \{l_{m,b} : (m, b) \in P\}$$

and

$$\begin{aligned} L(A) &= L_P(A) = \{l_{m,b}(a) = ma + b : (m, b) \in P, a \in A\} \\ E(L, A) &= |\{(l, l', a, a') \in L^2 \times A^2 : l(a) = l'(a')\}| \end{aligned} \quad (2.3)$$

For $L = L_P$, (2.3) becomes

$$E(L, A) = |\{ma + b = m'a' + b' : (m, b), (m', b') \in P, a, a' \in A\}|$$

We have the following result.

Theorem 2.4. *Let $P \subset R^2$ and $A \in R$. Let $L = L_P$. Then*

$$E(L, A) \leq \frac{1}{q^r} |L|^2 |A|^2 + q^{2r-1} |L| |A| \quad (2.4)$$

and

$$|L(A)| \gg \min \left\{ q^r, \frac{|L| |A|}{q^{2r-1}} \right\} \quad (2.5)$$

Proof. Define

$$Q = \{(m, b, a') : (m, b) \in P, a' \in A\}$$

$$\Pi = \{\pi : ax + y = m'z + b' : (m', b') \in P, a \in A\},$$

and note that $|Q| = |\Pi| = |L| |A|$, and also $E(L, A) = |I(Q, \Pi)|$. We therefore by Theorem 2.3 have

$$\begin{aligned} E(L, A) &= |I(Q, \Pi)| \\ &\leq \frac{1}{q^r} |Q| |\Pi| + q^{2r-1} |Q|^{\frac{1}{2}} |\Pi|^{\frac{1}{2}} \\ &= \frac{1}{q^r} |L|^2 |A|^2 + q^{2r-1} |L| |A| \end{aligned}$$

which proves the first part of the theorem. If we denote

$$r_{L(A)}(y) = |\{(m, b), a) \in P \times A : y = ma + b\}|,$$

then by the Cauchy-Schwarz inequality

$$\begin{aligned} |L|^2 |A|^2 &= \left(\sum_y r_{L(A)}(y) \right)^2 \\ &\leq |L(A)| \sum_y (r_{L(A)}(y))^2 \\ &= |L(A)| E(L, A) \\ &\ll |L(A)| \left(\frac{1}{q^r} |L|^2 |A|^2 + q^{2r-1} |L| |A| \right), \end{aligned}$$

therefore

$$|L(A)| \gg \min \left\{ q^r, \frac{|L| |A|}{q^{2r-1}} \right\}.$$

□

Proof of Theorem 1.1. Note that $BA + C = L_P(A)$ where $P = B \times C$ so that $L_P = L_{B \times C}$. Theorem 2.4 implies that

$$|BA + C| = |L_P(A)| \gg \min \left\{ q^r, \frac{|A| |B| |C|}{q^{2r-1}} \right\}. \quad (2.6)$$

If we take $A = B = C$ in (2.6), we simply get

$$|AA + A| \gg \min \left\{ q^r, \frac{|A|^3}{q^{2r-1}} \right\}$$

and when $q^r < \frac{|A|^3}{q^{2r-1}}$, i.e., $|A| > q^{r-\frac{1}{3}}$, we have $|AA + A| \gg q^r$ which proves the claim. □

3 Proof of Theorem 1.2

For the proof of Theorem 1.2 we will use the following Plünnecke-Ruzsa inequality.

Lemma 3.1. *Let A and B be finite subsets of an abelian group such that $|A + B| \leq K|A|$. Then for an arbitrary $0 < \delta < 1$ there is a nonempty set $X \subset A$ such that $|X| \geq (1 - \delta)|A|$ and for any integer k , one has*

$$|X + kB| < \left(\frac{K}{\delta} \right)^k |X|. \quad (3.1)$$

Proof of Theorem 1.2. Let $A^2 + A^2 = S$ and $|S| = K|A|$. we can use Lemma 3.1 to refine A to a large subset A' of A , and then for $k = 2$ we will get

$$|A'^2 + A'^2 + A'^2| \ll K^2|A|.$$

Since working with A' instead of A will not change the calculations in the end, we replace A with A' using the same notations as A and S . Let

$$\begin{aligned} E &= |\{c^2 + a^2 + b'^2 = c'^2 + a'^2 + b^2 : a, b, c, a', b', c' \in A\}| \\ &= |\{c^2 + a^2 - b^2 = c'^2 + a'^2 - b'^2 : a, b, c, a', b', c' \in A\}| \\ &= |\{c^2 + 2as - s^2 = c'^2 + 2a's' - s'^2 : s = a + b, s' = a' + b'\}| \end{aligned}$$

Hence $E = E(L, A)$ where $L = L_P$

$$P = \{(2s, c^2 - s^2) : s \in A + A, c \in A\}.$$

We can see $E(L, A)$ as a point-plane incidence in R^3 and Theorem 2.4 with $|L| \leq |A + A||A|$ gives

$$\begin{aligned} E = E(L, A) &\leq \frac{1}{q^r} |A + A|^2 |A|^2 |A|^2 + q^{2r-1} |A + A| |A| |A| \\ &= \frac{1}{q^r} |A + A|^2 |A|^4 + q^{2r-1} |A + A| |A|^2 \end{aligned}$$

From the Cauchy-Schwarz inequality, it follows that

$$\begin{aligned} |A|^6 &\leq |A^2 + A^2 + A^2| E \\ &\ll K^2 |A| E \\ &\leq \frac{|A^2 + A^2|^2}{|A|} \left\{ \frac{1}{q^r} |A + A|^2 |A|^4 + q^{2r-1} |A + A| |A|^2 \right\} \end{aligned} \quad (3.2)$$

Note that when $|A + A||A|^2 > q^{3r-1}$, the the first term in RHS of (3.2) dominates and we obtain

$$|A^2 + A^2| |A + A| \gg q^{\frac{r}{2}} |A|^{\frac{3}{2}}.$$

□

Acknowledgments. The author would like to thank Alex Iosevich and Jonathan Pakianathan for their valuable comments.

References

- [1] E. Aksoy Yazici, *Erdős Type Problems in Modules over Cyclic Rings*, 2015, Journal of Fourier Analysis and Applications, 10.1007/s00041-015-9417-y [1](#)
- [2] E. Aksoy Yazici, B. Murphy, M. Rudnev, I. Shkredov, *Growth Estimates in Positive Characteristic via Collisions*, Accepted IMRN, <http://arxiv.org/pdf/1512.06613.pdf>, 2015 [1](#), [2](#), [4](#)
- [3] J. Bourgain, *The sum-product theorem in \mathbb{Z}_q with q arbitrary*. J. Anal. Math. 106 (2008), 193. [1](#)
- [4] J. Bourgain, N. H. Katz, T. Tao, *A sum-product estimate in finite fields, and applications*, Geometric & Functional Analysis GAFA 14, no 1 (2004), 2757. [1](#)
- [5] P. Erdős, E. Szemerédi, *On sums and products of integers*. Studies in Pure Mathematics. To the memory of Paul Turán, Basel: Birkhuser Verlag, pp. 213-218. [1](#)
- [6] B. Murphy, O. Roche-Newton, I. D. Shkredov, *Variations on the sum-product problem*. SIAM Journal on Discrete Mathematics 29(1) (2015), 514540. [1](#)
- [7] O. Roche-Newton, M. Rudnev, I. D. Shkredov. *New sum-product type estimates over finite Fields*. Preprint, arXiv:1408.0542v3 [math.CO] 24 Jul 2015. [1](#)
- [8] G. Petridis, *Products of Differences in Prime Order Finite Fields* <https://arxiv.org/pdf/1602.02142v1.pdf>, 2016 [1](#)
- [9] M. Rudnev, *On the number of incidences between planes and points in three dimensions*, Preprint arXiv:1407.0426v4 [math.CO] 22 Sept 2014. [1](#)
- [10] M. Rudnev, I. Shkredov, S. Stevens, *On the Energy Variant of the Sum-Product Conjecture*, <https://arxiv.org/pdf/1607.05053.pdf>, 2016 [1](#)
- [11] P. V. Thang, L. A. Vinh, *Some combinatorial number theory problems over finite valuation rings*, <https://arxiv.org/pdf/1510.07218.pdf> [1](#), [3](#)
- [12] T. Tao, *The sum-product phenomenon in arbitrary rings*. Contrib. Discrete Math. 4 (2009), no. 2, 59-82. [1](#)
- [13] T. Tao, V. Vu. *Additive Combinatorics*. Cambridge University Press (2006). [1](#)